GOVERNMENT OF MAHARASHTRA
STATE COMMON ENTRANCE TEST CELL, MAHARASHTRA STATE, MUMBAI
8th Floor, New Excelsior Building, A.K. Nayak Road, Fort, Mumbai 400 001
Tele. No. - 022-22016157/53/59 Website -www.mahacet.org E-Mail-cetcell@mahacet.org

No.-2124/Forensic Security Audit/Ext./2026/2724. **Date :** 23/11/2026

EXTENSION NOTICE

Subject : **Extension of Last Date for Submission of Quotations for Forensic Security Audit and Grey-Box Vulnerability Assessment & Penetration Testing of CET Cell Examination Systems.**

Reference : **Quotation Invitation Notice No. No.-2124/Forensic Security Audit/2026/2678. Dated 16/11/2026.**

With reference to the above-mentioned Quotation Invitation Notice issued by the State Common Entrance Test Cell, Maharashtra State, Mumbai, inviting sealed quotations from eligible CERT-In Empanelled Information Security Auditing Organisations for conducting a Forensic Security Audit and Grey-Box Vulnerability Assessment & Penetration Testing of CET Cell Examination Systems, it is hereby informed that the last date for submission of quotations is extended as follows:

Particulars	**Revised Schedule**
Last Date of Submission of Quotation	**27/11/2026 up to 3:00 PM**
Quotation Opening Date	**27/11/2026 at 5:00 PM**

All other terms and conditions, eligibility criteria, and the Scope of Work prescribed in the original Quotation Invitation Notice shall remain unchanged.

Interested eligible agencies are requested to submit their sealed quotations along with the requisite eligibility documents within the extended deadline at the address mentioned in the original Quotation Invitation Notice.

This Extension Notice shall be read as an integral part of the original Quotation Invitation Notice.

Administrative Officer,
State Common Entrance Test Cell,
Maharashtra State, Mumbai.

Enclosure:

Annexure-I: Detailed Scope of Work for Forensic Security Audit and Grey-Box Vulnerability Assessment & Penetration Testing of CET Cell Examination Systems (20 Pages).

ANNEXURE – I

DETAILED SCOPE OF WORK
Forensic Security Audit and Grey-Box Vulnerability Assessment & Penetration Testing of CET Cell Examination Systems

Procuring Authority: State Common Entrance Test Cell, Maharashtra State, Mumbai.
Agency: CERT-In Empanelled Information Security Auditing Organisation.
Maximum Examination Centres: 5 (Five), as per directions of State CET Cell.
Audit Period: 01.03.2026 to 31.07.2026 (as specified in the Scope of Work).

---

1. BACKGROUND AND OBJECTIVES

The State Common Entrance Test Cell, Maharashtra State, conducts the Maharashtra Common Entrance Test (CET), a high-stakes, state-level entrance examination.

The CET examination ecosystem consists of multiple interconnected software applications, infrastructure and examination-related systems, including:

1. Exam Engine Software, Web Applications and APIs.
2. Hosting Infrastructure and Network.
3. Testing Centre Systems, including Candidate Nodes and Venue Servers.
4. Exam Response Sheet Server.

The State CET Cell intends to appoint an independent CERT-In Empanelled

Information Security Auditing Organisation to conduct a comprehensive Forensic Security Audit and Grey-Box Vulnerability Assessment and Penetration Testing of the above components.

The primary objective is to identify security vulnerabilities, assess the possibility of unauthorised access or data leakage, detect potential manipulation of examination-related information, verify the integrity of examination systems and evaluate the security controls implemented across the CET examination ecosystem.

1.1 Objectives

The audit shall cover the following objectives:

1. Identify and validate vulnerabilities in examination software, web applications, APIs and associated application components.
2. Examine the possibility of unauthorised access, privilege escalation, data leakage, data modification or deletion.
3. Assess the security of hosting infrastructure, operating systems, databases, network devices and security configurations.
4. Examine the security of examination systems installed at selected examination centres, including candidate nodes and venue servers.
5. Verify the security, confidentiality and integrity of examination response sheets stored and processed on the Exam Response Sheet Server.

6. Examine system logs, audit trails and available forensic evidence to identify suspicious activities, unauthorised access or possible data compromise.
7. Assess whether examination-related information can be accessed, copied, modified, deleted or manipulated by unauthorised users.
8. Identify gaps in security controls, access management, monitoring, logging and data protection.
9. Provide detailed findings, risk classification and corrective recommendations.
10. Submit the applicable CERT-In audit report and audit certificate.

2. AUDIT METHODOLOGY AND STANDARDS

2.1 Grey-Box Testing Approach

The audit shall be conducted using a Grey-Box approach, wherein the selected Agency shall be provided with limited technical information and controlled access to the systems under audit.

The State CET Cell shall provide, wherever available and applicable:

1. Test user accounts for different system roles, such as candidate, centre administrator, invigilator, observer, question setter, moderator, examination administrator and result processor.
2. High-level system architecture and network diagrams.
3. List of in-scope URLs, IP addresses, domains and servers.
4. API documentation, Swagger/OpenAPI specifications or Postman collections.
5. Examination client software installer/build.
6. One configured candidate node and local examination server image for laboratory testing.
7. Access to the Exam Response Sheet Server and its associated interfaces, databases and logs, subject to authorisation.
8. Details of relevant vendors, technical teams and system administrators.
9. A designated Single Point of Contact (SPOC) from the State CET Cell and the respective system vendor.

The Agency shall not be provided with source code or infrastructure administrator credentials unless specifically authorised by the State CET Cell for a particular audit activity.

2.2 Audit Standards and Guidelines

The Agency shall follow the latest applicable versions of the following standards and guidelines:

Sr. No.	Audit Area	Reference Standard / Guideline
1	Overall Security Audit	CERT-In Guidelines for Auditing and applicable CERT-In empanelment requirements
2	Web Application Security	OWASP Web Security Testing Guide (WSTG)

Sr. No.	Audit Area	Reference Standard / Guideline
3	Web Application Vulnerabilities	OWASP Top 10
4	Application Security Verification	OWASP ASVS Level 2
5	API Security	OWASP API Security Top 10
6	Desktop / Thick Client Security	OWASP Desktop Application Security guidance
7	Infrastructure and Network	NIST SP 800-115
8	Server and Database Hardening	CIS Benchmarks
9	Risk Classification	CVSS v3.1 or CVSS v4.0
10	Digital Forensic Examination	Recognised digital forensic evidence preservation and chain-of-custody practices

The Agency shall combine automated security testing with manual assessment. Every reported vulnerability shall be manually verified. Automated scanning output alone shall not be accepted as a confirmed security finding.

3. COMPONENT 1 – FORENSIC AUDIT OF EXAM ENGINE SOFTWARE, WEB APPLICATIONS AND APIs

The Agency shall conduct a comprehensive forensic security audit and Grey-Box of the CET Exam Engine Software, associated web applications, APIs and other application components.

The audit shall include, but not be limited to, the following activities:

3.1 Authentication and Session Management

1. Examine login and authentication mechanisms.
2. Check for brute-force attacks and credential-stuffing vulnerabilities.
3. Examine OTP and CAPTCHA implementation and possible bypass mechanisms.
4. Assess password reset and account recovery mechanisms.
5. Verify multi-factor authentication for privileged and administrative users, wherever implemented.
6. Examine session fixation, session hijacking and token manipulation vulnerabilities.
7. Verify session timeout, token expiry and logout mechanisms.
8. Examine the security of user authentication across different application roles.

3.2 Authorisation and Access Control

1. Verify role-based access control mechanisms.
2. Examine horizontal and vertical privilege escalation vulnerabilities.

3. Check Insecure Direct Object Reference (IDOR) vulnerabilities.
4. Verify whether candidates can access information belonging to other candidates.
5. Examine access restrictions for examination administrators, centre administrators, question setters, moderators and result processors.
6. Check whether unauthorised users can access restricted application modules.
7. Verify segregation of duties between different administrative roles.

3.3 Input Validation and Application Vulnerabilities

The Agency shall examine the application for:

1. SQL Injection.
2. NoSQL Injection.
3. OS Command Injection.
4. LDAP Injection.
5. Cross-Site Scripting (XSS).
6. XML External Entity (XXE) vulnerabilities.
7. Server-Side Request Forgery (SSRF).
8. Path Traversal vulnerabilities.
9. Insecure file upload and download mechanisms.
10. Improper input validation.
11. Insecure deserialization, where applicable.
12. Improper error handling and information disclosure.

3.4 Examination Business Logic Security

The Agency shall specifically examine examination-related business logic and workflow vulnerabilities, including:

1. Manipulation of examination timers.
2. Unauthorised modification of question sequence or question order.
3. Manipulation of candidate answer submissions.
4. Replaying or modifying previously submitted responses.
5. Unauthorised modification of examination responses after submission.
6. Unauthorised early access to question papers.
7. Unauthorised access to answer keys.
8. Manipulation of answer keys or answer evaluation mechanisms.
9. Unauthorised modification of candidate objections.
10. Manipulation of normalisation processes or result computation.
11. Unauthorised modification of examination-related transactions or payment status, where applicable.
12. Bulk extraction or scraping of candidate examination data.
13. Unauthorised access to examination administration functions.

3.5 API Security Audit

The Agency shall examine:

1. Broken Object Level Authorisation (BOLA).
2. Broken Function Level Authorisation (BFLA).
3. Mass assignment vulnerabilities.
4. Excessive data exposure.
5. Missing or inadequate API rate limiting.
6. Weak API authentication mechanisms.
7. Insecure JWT handling.
8. API key exposure.
9. Replay attacks.
10. Unauthorised API access.
11. Insecure API communication.
12. Unnecessary or exposed API endpoints.

3.6 Application Configuration and Dependency Security

1. Review application security configurations.
2. Examine HTTP security headers.
3. Verify TLS/SSL implementation.
4. Identify outdated or vulnerable libraries and dependencies.
5. Check for exposed credentials, tokens, API keys and secrets.
6. Identify debug mode exposure and unnecessary information disclosure.
7. Examine application error messages and stack traces.
8. Assess security of file storage and temporary directories.

3.7 Forensic Examination of Application Logs

The Agency shall examine available application logs and audit trails to identify:

1. Suspicious login activities.
2. Multiple failed authentication attempts.
3. Unauthorised administrative access.
4. Unusual user activities.
5. Unauthorised data downloads or exports.
6. Unusual access to candidate records.
7. Unauthorised modification or deletion of records.
8. Changes in examination configurations.
9. Unusual API access patterns.
10. Evidence of possible data leakage or unauthorised access.

3.8 Expected Outcome

The Agency shall provide a detailed report identifying application-level vulnerabilities, examination workflow risks, access control weaknesses, data exposure risks and any forensic indicators of unauthorised activity.

4. COMPONENT 2 – FORENSIC AUDIT OF HOSTING INFRASTRUCTURE AND NETWORK

The Agency shall conduct a comprehensive forensic security audit and of the infrastructure and network supporting the CET examination platform.

4.1 External Network Security Audit

1. Identify exposed IP addresses, ports and services.
2. Perform service and version identification.
3. Identify vulnerable internet-facing services.
4. Examine firewall and perimeter security configurations.
5. Assess Web Application Firewall (WAF) security posture.
6. Identify publicly accessible administrative interfaces.
7. Examine exposed databases, storage services and management ports.
8. Identify unnecessary services and insecure protocols.
9. Assess protection mechanisms against network-based attacks.

Actual Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks shall not be performed.

4.2 Internal Network Security Audit

1. Examine internal network architecture.
2. Assess network segmentation between web, application, database and management networks.
3. Identify unauthorised access paths between network segments.
4. Examine access restrictions between servers.
5. Assess lateral movement possibilities.
6. Identify unnecessary network connectivity.
7. Review internal firewall rules and access control lists.
8. Examine remote administration and VPN access mechanisms.

4.3 Server Security Audit

The Agency shall examine:

1. Operating system security configuration.
2. Operating system patch levels.
3. Security updates and vulnerability status.
4. Unnecessary services and processes.
5. Default accounts and passwords.
6. Privileged user accounts.
7. Administrative access mechanisms.
8. Remote access configurations.
9. File and directory permissions.
10. System logging and monitoring.

11. Endpoint security and protection mechanisms.

4.4 Database Security Audit

1. Review database security configurations.
2. Examine database user accounts and privileges.
3. Verify role-based database access.
4. Identify excessive privileges.
5. Examine database exposure to external networks.
6. Verify database encryption mechanisms, wherever applicable.
7. Examine database audit logs.
8. Assess backup security.
9. Identify database configuration weaknesses.
10. Review access to sensitive examination-related information.

4.5 Network Device and Security Configuration Audit

1. Review firewall configurations.
2. Examine VPN security.
3. Assess network device administration access.
4. Review access control lists.
5. Examine insecure protocols.
6. Review network logging and monitoring.
7. Assess security monitoring and alerting mechanisms.

4.6 Forensic Examination of Infrastructure Logs

The Agency shall review available:

1. Operating system logs.
2. Server access logs.
3. Database audit logs.
4. Firewall logs.
5. WAF logs.
6. VPN logs.
7. Network device logs.
8. Security monitoring logs.
9. Administrative activity logs.

The objective shall be to identify suspicious access, unauthorised changes, unusual network traffic, possible data exfiltration, privilege escalation and other indicators of compromise.

4.7 Expected Outcome

The Agency shall provide a detailed infrastructure security assessment identifying vulnerabilities, misconfigurations, exposed services, unauthorised access possibilities and security weaknesses in the hosting and network environment.

5. COMPONENT 3 – FORENSIC AUDIT OF TESTING CENTRE SYSTEMS: CANDIDATE NODES AND VENUE SERVERS

The Agency shall conduct forensic security audits of examination systems installed at selected CET examination centres.

5.1 Number of Examination Centres

1. The State CET Cell shall select a maximum of five (5) examination centres for this audit.
2. The number of centres shall not exceed five under this assignment.
3. The final number of centres shall be specified in the Work Order.
4. Centres may be located anywhere within Maharashtra State.
5. The State CET Cell shall provide the selected centre list and addresses at least 10 days before the scheduled visits, wherever practicable.

5.2 Sampling at Each Examination Centre

At each selected examination centre, the Agency shall audit:

1. All relevant local examination/venue server(s) within the approved scope.
2. Five (5) candidate nodes selected on the spot by the Agency in coordination with the State CET Cell representative.

Therefore, the maximum planned candidate-node sampling shall be 25 nodes across five centres.

5.3 Venue Server Security Audit

The Agency shall examine:

1. Operating system security configurations.
2. Application installation and configuration.
3. Patch levels and security updates.
4. Unauthorised services and processes.
5. User accounts and privileged access.
6. Remote administration mechanisms.
7. File and directory permissions.
8. Local data storage.
9. Security logs and audit trails.
10. Network connectivity and access controls.
11. Unauthorised software installation.
12. Possible tampering with examination server configurations.

5.4 Candidate Node Security Audit

The Agency shall examine the five selected candidate nodes at each centre for:

1. Operating system vulnerabilities.
2. Unauthorised software and applications.

3. Local administrator privileges.
4. USB and removable media access controls.
5. Endpoint security configuration.
6. Antivirus and endpoint protection status.
7. Security patch levels.
8. Local data storage and temporary files.
9. Examination client installation integrity.
10. Unauthorised configuration changes.
11. Local logs and system activity.
12. Possible manipulation of examination client software.

5.5 Examination Client Software Audit

The Agency shall assess:

1. Integrity of the examination client installation.
2. Possibility of unauthorised modification of client software.
3. Security of client-server communication.
4. Unauthorised access to local examination files.
5. Exposure of credentials or sensitive configuration data.
6. Possibility of manipulating examination activities through the candidate node.
7. Security of software updates and configuration changes.
8. Possibility of bypassing client-side security controls.

5.6 Centre Network Security Audit

The Agency shall examine:

1. Network connectivity between candidate nodes and venue servers.
2. Network segmentation.
3. Access restrictions between examination systems.
4. Unauthorised devices connected to the examination network.
5. Possibility of unauthorised access to venue servers.
6. Communication between centre systems and central examination infrastructure.
7. Network logging and monitoring.

5.7 Forensic Examination at Examination Centres

The Agency shall review available logs and system artefacts to identify:

1. Suspicious user activities.
2. Unauthorised software execution.
3. Unauthorised file transfers.
4. Modification of examination client files.
5. Unauthorised access to local examination data.
6. Suspicious network connections.
7. Changes to examination configurations.

8. Evidence of possible tampering or compromise.

5.8 Centre Visit Conditions

1. Centre visits shall be conducted only on non-examination days.
2. The audit shall not disturb any scheduled examination or mock test.
3. A State CET Cell representative shall be present during each visit.
4. No audit tool shall be installed on centre systems without prior written approval.
5. All temporary audit tools, files and test configurations shall be removed before the Agency leaves the centre.
6. The Agency shall ensure that the examination systems are restored to their original operational state after testing.

5.9 Expected Outcome

The Agency shall provide a separate centre-wise forensic security audit report covering venue servers, candidate nodes, examination client software and network security.

6. COMPONENT 4 – FORENSIC AUDIT OF EXAM RESPONSE SHEET SERVER

The Agency shall conduct a dedicated Forensic Security Audit and Grey-Box of the CET Exam Response Sheet Server and all associated application, database, storage and communication components.

The purpose of this audit is to verify the confidentiality, integrity, authenticity, availability and traceability of candidate examination response sheets.

The audit shall cover the complete lifecycle of examination response sheets, including receipt, transfer, storage, processing, retrieval, access, export, backup and retention.

6.1 Server Architecture and Configuration Audit

The Agency shall:

1. Review the architecture of the Exam Response Sheet Server.
2. Examine application and database components.
3. Review data flow between the Exam Engine and Response Sheet Server.
4. Identify all interfaces used for receiving and retrieving response sheets.
5. Review server configuration and security settings.
6. Examine network exposure and access restrictions.
7. Review dependencies and third-party integrations.
8. Identify potential security weaknesses in the architecture.

6.2 Authentication and Access Control Audit

The Agency shall examine:

1. Authentication mechanisms used to access response sheets.

2. Role-based access control.
3. Administrative and privileged user access.
4. Database user privileges.
5. Service accounts and application credentials.
6. Segregation of duties.
7. Unauthorised access to candidate response sheets.
8. Access restrictions between different examination centres.
9. Access restrictions between different candidates.
10. Possibility of unauthorised bulk access or downloads.

6.3 Response Sheet Data Transfer Security

The Agency shall assess:

1. Security of response-sheet transmission from examination centres or examination servers.
2. Security of communication between the Exam Engine and Response Sheet Server.
3. Encryption of response-sheet data during transmission.
4. Authentication of systems transferring response sheets.
5. Possibility of interception or unauthorised modification during transmission.
6. Replay or duplicate submission vulnerabilities.
7. Unauthorised replacement of response-sheet files.
8. Integrity verification during transfer.
9. Failure handling and recovery mechanisms.

6.4 Response Sheet Storage Security

The Agency shall examine:

1. Security of response-sheet storage locations.
2. Database and file-storage access permissions.
3. Encryption of stored response sheets, wherever implemented.
4. Access to temporary files and cache.
5. Backup storage security.
6. Unauthorised file access.
7. Unauthorised file modification or deletion.
8. Exposure through direct URLs or storage interfaces.
9. Access to archived response sheets.

6.5 Response Sheet Integrity and Tampering Audit

The Agency shall specifically examine whether examination response sheets can be modified, replaced or manipulated after submission.

The audit shall include:

1. Verification of available hash/checksum mechanisms.
2. Digital signature implementation, wherever applicable.

3. Verification of response-sheet authenticity.
4. Examination of timestamps and submission metadata.
5. Verification of integrity during storage and retrieval.
6. Detection of duplicate or altered response sheets.
7. Possibility of replacing one candidate's response sheet with another.
8. Possibility of modifying candidate responses after submission.
9. Possibility of unauthorised deletion of submitted response sheets.
10. Availability of audit trails to identify modifications.

6.6 Response Sheet Application and API Security

The Agency shall examine:

1. Authentication of response-sheet APIs.
2. Authorisation of response-sheet retrieval requests.
3. Unauthorised access to response-sheet endpoints.
4. Insecure direct object references.
5. Bulk response-sheet download vulnerabilities.
6. API parameter manipulation.
7. Unauthorised response-sheet export.
8. Insecure file upload/download mechanisms.
9. Exposure of response-sheet information through error messages or application logs.
10. Weak API keys, tokens or authentication mechanisms.

6.7 Response Sheet Processing and Downstream Integration

The Agency shall examine the security of interfaces and processes through which response sheets are:

1. Retrieved from the response-sheet server.
2. Processed by examination-related applications.
3. Shared with authorised evaluation or result-processing systems.
4. Exported for verification or administrative purposes.
5. Archived for future reference.

The audit shall identify whether unauthorised users or systems can modify, substitute, delete or manipulate response sheets during these processes.

6.8 Logging and Audit Trail Verification

The Agency shall verify whether the system maintains sufficient audit trails for:

1. Response sheet creation or receipt.
2. Upload and transfer.
3. Storage.
4. Access and viewing.
5. Download and export.
6. Modification.

7. Deletion.
8. Administrative access.
9. Database operations.
10. System configuration changes.

The Agency shall also examine whether logs capture:

1. User or system identity.
2. Date and timestamp.
3. Source IP or system identity, where available.
4. Action performed.
5. Response or outcome.
6. Record or file reference.
7. Administrative activity.

The Agency shall examine whether logs can be modified, deleted or bypassed by unauthorised users.

6.9 Backup, Retention and Deletion Security

The Agency shall examine:

1. Security of response-sheet backup mechanisms.
2. Access control over backup repositories.
3. Integrity of backup data.
4. Response-sheet retention mechanisms.
5. Archival security.
6. Deletion mechanisms.
7. Possibility of unauthorised deletion or alteration.
8. Availability of recovery and restoration mechanisms.

6.10 Forensic Examination and Data Leakage Assessment

The Agency shall examine available application, database, storage, server and network logs to identify:

1. Suspicious access to response sheets.
2. Unauthorised bulk downloads.
3. Unusual access patterns.
4. Unauthorised data exports.
5. Suspicious administrative activities.
6. Modification or deletion of response sheets.
7. Unauthorised access from external systems.
8. Possible data leakage or exfiltration.
9. Indicators of compromise.

The Agency shall prepare a timeline of suspicious activities wherever sufficient logs and evidence are available.

6.11 Expected Outcome

The Agency shall provide a dedicated forensic audit report covering:

1. Security of the Exam Response Sheet Server.
2. Confidentiality of candidate response sheets.
3. Integrity and authenticity of response-sheet data.
4. Access control and administrative privileges.
5. Data transfer and storage security.
6. Possibility of unauthorised modification, replacement or deletion.
7. Audit logging and traceability.
8. Data leakage and possible compromise indicators.
9. Security gaps and recommended corrective measures.

Important: The Agency shall not download or retain bulk actual candidate response sheets. Synthetic, masked or specifically authorised sample data shall be used wherever feasible. Any access to actual candidate response sheets required for validation shall be minimised, logged and approved in writing by the State CET Cell.

7. DIGITAL FORENSIC EVIDENCE COLLECTION AND HANDLING

In addition to the component-wise audit, the Agency shall follow proper forensic evidence handling practices wherever evidence collection is authorised.

The Agency shall:

1. Identify relevant system logs, application logs, database logs and security artefacts.
2. Record the source and custodian of each collected evidence item.
3. Record the date, time and method of collection.
4. Generate integrity hashes, preferably SHA-256, for collected evidence files where technically feasible.
5. Maintain an evidence register and chain-of-custody documentation.
6. Preserve original evidence without unauthorised modification.
7. Prepare event timelines wherever evidence permits.
8. Distinguish confirmed findings from indicators of compromise and technical observations.
9. Identify limitations arising from missing logs, incomplete retention or unavailable evidence.
10. Immediately report suspected active compromise or ongoing data leakage to the designated State CET Cell officer.

The assignment shall cover forensic security examination within the approved audit scope. Full-scale incident response, recovery operations or legal attribution shall require separate written authorisation.

8. GENERAL TESTING CONDITIONS AND RESTRICTIONS

The Agency shall comply with the following conditions:

1. All audit activities shall be authorised in writing by the State CET Cell.
2. Testing shall be limited to the approved systems, IP addresses, URLs, applications and examination centres.
3. Testing shall not disrupt live examination activities.
4. Actual DoS/DDoS, stress or load testing shall not be conducted.
5. Destructive testing shall not be permitted.
6. No examination question paper, answer key, candidate response or response sheet shall be altered or deleted during testing.
7. No malware, ransomware or persistence mechanism shall be installed or executed.
8. No unauthorised tools shall be installed on production or centre systems.
9. Proof-of-concept activities shall be performed using safe methods and synthetic or masked data wherever possible.
10. The Agency shall maintain a record of all testing activities.
11. Critical and High vulnerabilities shall be immediately communicated to the designated State CET Cell SPOC.
12. All test files, tools and temporary configurations shall be removed after completion of testing.

9. DELIVERABLES AND TIMELINES

The selected Agency shall submit the following deliverables:

Sr. No.	Deliverable	Description	Timeline
D1	Audit Plan and Rules of Engagement	Detailed methodology, testing approach, tools, test cases, audit schedule, team details and escalation matrix covering all four components.	Within 7 working days from Work Order.
D2	Forensic Audit of Exam Platform, Infrastructure and Response Sheet Server	Completion of Component 1, Component 2 and Component 4.	Within 5 weeks from sharing all required system details and access.
D3	Forensic Audit of Examination Centres	Centre-wise audit of venue servers and five candidate nodes at each selected centre, up to a maximum of five centres.	As per mutually agreed schedule and availability of centres.
D4	Draft Forensic Report	Detailed findings, vulnerabilities, forensic observations, risk classification and recommendations.	Within 10 working days from completion of relevant testing.

Sr. No.	Deliverable	Description	Timeline
D5	Final Forensic Audit Report and Certificate	Final report incorporating Department comments and applicable CERT-In audit certificate.	Within 7 working days from receipt of consolidated Department comments.
D6	Closing Presentation	Presentation of major risks, Critical and High vulnerabilities and priority corrective measures to senior officials.	Along with D5.

9.1 Report Format

The draft and final reports shall include:

1. Executive summary.
2. Overall security posture.
3. Scope and methodology.
4. System components audited.
5. Detailed findings with unique finding IDs.
6. Affected system, application, server or component.
7. Vulnerability description.
8. CVSS score and severity.
9. Business impact in the context of CET.
10. Steps to reproduce or validate the finding.
11. Supporting screenshots, logs or other evidence, with personal data masked.
12. Recommended corrective actions.
13. Summary of findings by severity and component.
14. List of test cases performed with Pass/Fail/Not Applicable/Not Tested status.
15. Tools and versions used.
16. Names and details of auditors.
17. Forensic evidence register, wherever applicable.
18. Open findings and residual risks.
19. Limitations and exclusions.

The report shall clearly state the security status of the systems as on the date of testing.

10. AUDIT AGENCY ELIGIBILITY AND TEAM REQUIREMENTS

The selected Agency shall satisfy the following requirements:

1. The Agency must be a CERT-In Empanelled Information Security Auditing Organisation on the bid submission date.
2. The Agency shall maintain valid CERT-In empanelment throughout the contract period.

3. Loss of required empanelment during the contract period may be treated as grounds for termination, subject to contract conditions.
4. The Agency shall deploy an experienced audit team having expertise in application security, API security, network security, infrastructure security and digital forensic examination.
5. The team shall include at least one Project Lead having a minimum of eight (8) years of relevant information security audit experience.
6. All deployed team members shall be Indian nationals.
7. The bidder shall submit details of the proposed audit team, qualifications, certifications and relevant experience.
8. Any change in key audit personnel shall require prior written approval from the State CET Cell.
9. Replacement personnel shall have qualifications and experience equal to or better than the personnel being replaced.

11. CONFIDENTIALITY AND DATA HANDLING

The selected Agency shall comply with the following requirements:

1. The Agency and every team member shall sign a Non-Disclosure Agreement (NDA) before receiving any Department information or system access.
2. All audit activities shall be performed from within India.
3. No Department data, examination data, response sheets, audit reports or evidence shall be stored or processed outside India.
4. Audit reports and evidence shall be shared only through encrypted communication channels with authorised Department officers.
5. Candidate personal information and examination response data shall be accessed only to the minimum extent required for authorised testing.
6. All collected evidence shall be protected against unauthorised access, modification, disclosure or loss.
7. Any accidental disclosure or suspected compromise of Department data in the Agency's custody shall be immediately reported to the State CET Cell.
8. The Agency shall not publish, present or refer to any audit finding or engagement without prior written approval from the State CET Cell.
9. Within fifteen (15) days of final report acceptance, the Agency shall securely delete all Department data, credentials, temporary files and evidence from its systems, subject to any legally mandated retention disclosed to and approved by the Department.
10. The Agency shall submit a written certificate confirming deletion of the Department's data.

11. ROLES AND RESPONSIBILITIES

State CET Cell / Department	Selected Audit Agency
Provide system architecture, available technical documentation and asset details.	Prepare audit methodology, testing plan and Rules of Engagement.
Provide authorised test accounts and controlled access.	Conduct the audit strictly within the approved scope.
Coordinate with relevant system vendors and technical teams.	Deploy qualified and experienced audit personnel.
Provide access to relevant logs and system artefacts, subject to availability and authorisation.	Perform forensic examination and maintain evidence records.
Identify and coordinate up to five examination centres.	Conduct centre-wise audit of venue servers and five candidate nodes per centre.
Nominate Department SPOCs and representatives.	Maintain coordination with designated Department officers.
Review draft audit reports and provide consolidated comments.	Submit final reports and applicable audit certificates.
Take necessary action for remediation of identified vulnerabilities.	Provide corrective recommendations and explain identified risks.

13. COMMERCIAL QUOTATION STRUCTURE / BILL OF QUANTITIES (BOQ)

The bidder shall submit the financial quotation according to the following structure:

Sr. No.	Description	Unit	Quantity	Amount (₹)
1	Forensic Audit of Exam Engine Software, Web Applications and APIs; Forensic Audit of Hosting Infrastructure and Network; Forensic Audit of Exam Response Sheet Server; and Forensic Audit of Testing Centre Systems, including venue server(s) and five candidate nodes per centre (Maximum 5 centres).	Included in consolidated rate	1	
2	Applicable GST	As applicable	—	
3	**Total Quoted Amount**	—	—	

13.1 Commercial Conditions

1. The bidder shall quote one consolidated lump-sum rate covering Sr. No. 1.
2. The number of examination centres shall not exceed five (5).
3. The per-centre rate shall include travel, accommodation, local conveyance, audit tools and incidental expenses.
4. Payment for the audit shall be based upon the Final Report submission.
5. No additional amount shall be payable towards travel or accommodation for the centre visits unless expressly provided in the tender conditions.

14. COMPLETION AND ACCEPTANCE CRITERIA

The assignment shall be considered completed upon fulfilment of the following:

1. Completion of the authorised forensic security audit of all applicable components.
2. Completion of centre audits for the number of centres specified in the Work Order, not exceeding five.
3. Submission of the draft and final forensic audit reports.
4. Submission of the detailed vulnerability register.
5. Submission of the forensic evidence register and chain-of-custody documentation, wherever applicable.
6. Submission of the applicable CERT-In audit certificate.
7. Submission of component-wise and centre-wise findings.
8. Submission of recommendations for remediation of identified vulnerabilities.
9. Completion of the closing presentation.
10. Submission of the data deletion certificate.

The scope does not include implementation of security fixes, application redevelopment, infrastructure modification or re-testing after remediation unless separately authorised by the State CET Cell.

15. GENERAL CONDITIONS

1. The Agency shall comply with applicable Government of India and Government of Maharashtra instructions, CERT-In requirements and State CET Cell security policies.
2. The Agency shall maintain independence and disclose any conflict of interest.
3. The Agency shall not subcontract any part of the audit without prior written approval from the State CET Cell.
4. All findings, reports and audit artefacts prepared specifically under this engagement shall be handed over to the State CET Cell.
5. Any change in scope shall require written approval from the State CET Cell.
6. The Agency shall maintain confidentiality of all information received during the assignment.

7. The State CET Cell reserves the right to verify the qualifications and experience of the proposed audit team.
8. The audit shall be conducted in a manner that does not affect the availability, integrity or functioning of CET examination systems.

16. SUMMARY OF SCOPE COMPONENTS

Sr. No.	Forensic Audit Component	Coverage
1	Forensic Audit of Exam Engine Software, Web Applications and APIs	Examination applications, APIs, authentication, access control, business logic, data protection and application logs.
2	Forensic Audit of Hosting Infrastructure and Network	Hosting servers, operating systems, databases, network devices, firewalls, infrastructure configurations and logs.
3	Forensic Audit of Testing Centre Systems – Candidate Nodes and Venue Servers	Maximum 5 centres; all relevant local venue servers and 5 candidate nodes per centre (maximum 25 candidate nodes).
4	Forensic Audit of Exam Response Sheet Server	Response-sheet receipt, storage, transfer, processing, integrity, access control, logging, backup and data leakage assessment.

End of Annexure – I